



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/868,417	10/23/2001	Charles Cameron Lindquist	12143/1	1411
26646 7590 07/16/2010 KENYON & KENYON LLP ONE BROADWAY NEW YORK, NY 10004				
EXAMINER BIAGINI, CHRISTOPHER D				
ART UNIT 2442		PAPER NUMBER		
MAIL DATE 07/16/2010		DELIVERY MODE PAPER		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents  
United States Patent and Trademark Office  
P.O. Box 1450  
Alexandria, VA 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

**BEFORE THE BOARD OF PATENT APPEALS  
AND INTERFERENCES**

Application Number: 09/868,417  
Filing Date: October 23, 2001  
Appellant(s): LINDQUIST, CHARLES CAMERON

\_\_\_\_\_  
Aaron Grunberger  
For Appellant

**EXAMINER'S ANSWER**

This is in response to the appeal brief filed May 10, 2010 appealing from the Office action mailed April 9, 2009.

**(1) Real Party in Interest**

The examiner has no comment on the statement, or lack of statement, identifying by name the real party in interest in the brief.

**(2) Related Appeals and Interferences**

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

**(3) Status of Claims**

The following is a list of claims that are rejected and pending in the application:

Claims 59-61, 63-120, 123, and 124.

**(4) Status of Amendments After Final**

The examiner has no comment on the appellant's statement of the status of amendments after final rejection contained in the brief.

**(5) Summary of Claimed Subject Matter**

The examiner has no comment on the summary of claimed subject matter contained in the brief.

**(6) Grounds of Rejection to be Reviewed on Appeal**

The examiner has no comment on the appellant's statement of the grounds of rejection to be reviewed on appeal. Every ground of rejection set forth in the Office action from which the appeal is taken (as modified by any advisory actions) is being maintained by the examiner except for the grounds of rejection (if any) listed under the subheading "WITHDRAWN REJECTIONS." New grounds of rejection (if any) are provided under the subheading "NEW GROUNDS OF REJECTION."

#### **(7) Claims Appendix**

The examiner has no comment on the copy of the appealed claims contained in the Appendix to the appellant's brief.

#### **(8) Evidence Relied Upon**

6,271,752	Vaios	8-2001
6,061,650	Malkin	5-2000
6,453,348	Barnier	9-2002
6,496,862	Akatsu	12-2002
6,044,349	Tolopka	3-2000
5,948,059	Woo	9-1999
5,809,311	Jones	9-1998
6,014,746	Krehnke	1-2000
5,668,929	Foster	9-1997
6,178,433	Nakamura	1-2001

5,940,074	Britt	8-1999
6,032,202	Lea	2-2000
5,497,430	Sadovnik	3-1996
6,445,694	Swartz	9-2002
6,108,300	Coile	8-2000
6,088,330	Bruck	7-2000
5,649,014	Koopman	7-1997
5,892,758	Agyroudis	4-1999
6,243,596	Kikinis	6-2001
5,956,487	Venkatraman	9-1999

#### **(9) Grounds of Rejection**

The following ground(s) of rejection are applicable to the appealed claims:

#### ***Claim Rejections - 35 USC § 112***

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 59-61, 63-120, 123, and 124 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled

in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claims 59 and 124 recite the new limitation “at least one communications server...determines which one of said environments said authorization data indicates authority to access.” The most relevant part of the instant application appears to be page 9, under the heading “Remote Operation.” This section recites that the user first “enter[s] a URL associated with the HTML page they wish to access” (p. 9, lines 15-16), then completes a “login procedure associated with the HTML pages in question” (p. 9, line 19). Once the user is authenticated, the user is “permitted access to the HTML page requested” (p. 9, line 21). In addition, following the authentication process, “the records associated with the user, detailing connection parameters for the user premises, are retrieved from a database 18 in the provider network” (p. 9, lines 22-24). Merely retrieving records “detailing connection parameters” from database 18 is not the same as the “at least one communications server...determin[ing] which one of said environments said authorization data indicates authority to access.”

Any claim not specifically addressed above is rejected at least for incorporating the deficiencies of claim 59.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 59, 64-68, 76, 78-81, 88, 89, 91-94, 102, 104, 105, 109, 110, 112-114, 117, and 123 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaios (US Patent No. 6,271,752) in view of Malkin et al. (US Patent No. 6,061,650, hereinafter "Malkin"), and further in view of Barnier et al. (US Patent No. 6,453,348, hereinafter "Barnier").

Regarding claim 59, note that the preamble has been given patentable weight as it is relied upon by the body of the claim.

Vaios shows a system for remote access of environments (surveillance areas 4: see col. 3, lines 24-27; col. 9, lines 32-35) comprising:

- an Internet browser (remote computer system 16: see col. 4, lines 5-7);
- a network located external to said environments environment and accessible via said Internet browser (communications network 6: see col. 4, lines 30-42);
- a plurality of connection gateways, each of said environments having located therein a different one or more of said connection gateways (network interfaces 14: see Fig. 1 and col. 3, lines 24-27).

Vaios further shows controlling or monitoring operation of at least one service in said environment (see col. 7, lines 39-56, and col. 9, lines 49-61, with said connection gateway providing access to information contained within the environment directly to said Internet browser (see col. 7, lines 39-56).

Vaios does not explicitly show:

- that the network is an extranet;

- at least one communications server located in said extranet and adapted to interconnect on-demand with said connection gateways;
- wherein responsive to accessing a predetermined address by said Internet browser on said extranet, in which accessing said Internet browser provides authorization data, one of said at least one communications server subsequently:
  - determines which one of said environments said authorization data indicates authority to access; and
  - creates a new communications session between said communications server and one of said connection gateways, which is located in said environment, with said connection gateway subsequently providing access to information contained within the environment directly to said Internet browser.

Malkin shows:

- at least one communications server located in a network and adapted to interconnect on-demand with connection gateways (Remote Access Server 22: see col. 2, lines 13-17);
- wherein responsive to accessing a predetermined address by said Internet browser on said network (comprising the RAS's telephone number: see col. 3, lines 22-25), in which accessing said Internet browser provides authorization data (comprising a login name made up of a user name part and a domain specific part: see col. 3, lines 40-47), one of said at least one communications server subsequently:



- determines which one of said environments said authorization data indicates authority to access (comprising using the domain part of the login name to look up the address of a gateway interface and authentication server for a particular home network: see col. 3, line 48 to col. 4, line 14); and
- creates a new communications session between said communications server and one of said connection gateways (comprising a tunnel to a gateway: see col. 5, lines 35-46), which is located in said environment (see col. 5, line 65 to col. 6, line 3), with said connection gateway subsequently providing access to information contained within the environment directly to said Internet browser (see col. 6, lines 30-35).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Vaios with the communication server, authorization, and session establishment taught by Malkin in order to allow a user at a mobile remote node to seamlessly access his home environment (see Malkin, col. 1, lines 38-40).

Barnier shows a network comprising an extranet (see col. 2, lines 33-52). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaios with the extranet taught by Barnier in order to establish a highly secure environment in which to provide for monitoring (see Barnier, col. 4, lines 41-53).

Regarding claim 64, the combination shows the limitations of claim 59 as applied above, and further shows wherein said communications communication server utilizes a

telecommunications network to interconnect with said connection gateway (see Malkin, col. 3, lines 25-30 and Vaios, Fig. 1, network 6).

Regarding claim 65, the combination shows the limitations of claim 59 as applied above, and further shows wherein authentication to access said extranet is required only once per Internet browser session (see Malkin, col. 5, lines 47-50).

Regarding claim 66, the combination shows the limitations of claim 59 as applied above, and further shows wherein said extranet is a private network overlaid on forms part of the Internet (see Barnier, col. 1, lines 57-66) and said communications server is located within a local telephone call radius of the environment, thus providing lowest cost PSTN access from or to the environment (see Malkin, col. 3, lines 27-30).

Regarding claim 67, the combination shows the limitations of claim 59 as applied above, and further shows wherein additional interface pages accessible via said browser are provided on said extranet for each user of said system, said pages adaptable to provide details of a current status of one of said environments which is associated with environment of said user (see Vaios, col. 7, line 63 – col. 8, line 17 and col. 9, lines 49-64).

Regarding claim 68, the combination shows the limitations of claim 59 as applied above, and further shows wherein said extranet provides a user premises e-mail facility, and

automatically raises connection in a pre- programmed fashion to said connection gateway and transfers user e-mail to said connection gateway (see Barnier, col. 3, lines 62-65).

Regarding claim 76, the combination shows the limitations of claim 59 as applied above, and further shows further comprising a control terminal interconnected to said connection gateway (comprising a remote computer at end user locations 8: see Vaios, col. 4, lines 5-14).

Regarding claim 78, the combination shows the limitations of claim 76 as applied above, and further shows wherein the control terminal is connected to said connection gateway in a wireless manner (see Vaios, col. 4, lines 30-43).

Regarding claim 79, the combination shows the limitations of claim 78 as applied above, and further shows wherein the control terminal is powered by rechargeable batteries, allowing the control terminal mobility within the range of wireless transmitters attached to said environment (implicitly disclosed as a component of a beeper: see Vaios, col. 4, lines 5-14).

Regarding claim 80, the combination shows the limitations of claim 76 as applied above, and further shows wherein the control terminal is of reduced handheld size, so that it can operate as a universal premises remote control (note that it would be obvious to reduce a terminal to handheld size in order to make it more portable, see also Vaios, col. 4, lines 5-14).

Regarding claim 81, the combination shows the limitations of claim 76 as applied above, and further shows wherein the control terminal includes a digital camera, microphone and speaker, and video conferencing software, thus allowing the control terminal to be used as a videophone, through a standard browser interface (see Vaios, col. 9, lines 49-63).

Regarding claim 88, the combination shows the limitations of claim 59 as applied above, and further shows wherein said connection gateways form nodes of a distributed computing environment that may be allocated by said extranet on a demand basis (see Malkin, col. 3, lines 22-25 and note that resources are allocated upon the user's request).

Regarding claim 89, the combination shows the limitations of claim 59 as applied above, and further shows the system providing information access across at least two networks, wherein: said extranet is a first network having a first network access controller (comprising a router: see Barnier, Fig. 3); said environment is a second network having a second network access controller (comprising a router: see Vaios, col. 6, lines 54-60); said system further comprises comprising a user access browser located on said first network for locating and examining information on said first and second networks by means of network address locators (for example, phone numbers: see Malkin, col. 3, lines 21-30); and when a predetermined location on said first network is accessed, said first network access controller initiates an establishment of a network connection to said second network access controller so as to provide for a temporary interconnection of said first network to said second network, said system thereby

providing a seamless access to information stored on said second network from said user access browser (see Malkin, col. 5, lines 35-39).

Regarding claim 91, the combination shows the limitations of claim 59 as applied above, and further shows storage means forming part of said extranet (see Barnier, Fig. 3, storage 60 and col. 4, lines 53-56); and a device activating a security condition upon the occurrence of a predetermined event; wherein, upon the occurrence of said predetermined event, said device notifies said connection gateway and transfers event information on said predetermined event to said connection gateway and said connection gateway establishes an interconnection with said communications server and transfers said event information via said communications server to said storage means for later interrogation by a user of said system and initiates predetermined alert notification actions (see Vaio, col. 8, lines 56-58 and Barnier, col. 5, lines 18-23).

Regarding claim 92, the combination shows the limitations of claim 91 as applied above, and further shows wherein said device includes alert conditions which are forwarded to said connection gateway, wherein it is qualified with a pre-programmed enable, and if the result is TRUE, an event is generated, whereupon said connection gateway establishes a connection with said communications server (see Vaio, col. 8, lines 56-58 and Barnier, col. 5, lines 18-23).

Regarding claim 93, the combination shows the limitations of claim 92 as applied above, and further shows wherein said device is a security sensor device, said system is a security

system, said event is a security alarm event, and said data is surveillance data or security alert data (see Vaios, col. 8, lines 36-47).

Regarding claim 94, the combination shows the limitations of claim 93 as applied above, and further shows wherein surveillance data related to said alarm event is uploaded to said extranet for secure storage accessible upon interrogation by a user (see Barnier, col. 5, lines 19-24).

Regarding claim 102, the combination shows the limitations of claim 92 as applied above, and further shows wherein user data storage on said extranet for storing event data associated with said environment is allocated virtually (see Barnier, col. 5, lines 19-24).

Regarding claim 104, the combination shows the limitations of claim 92 as applied above, and further shows wherein said extranet includes a user contact database which includes preferred contact methods, allowing automatic contact mechanisms to be associated with alarm condition, including use of e-mail, pager, computer generated voice message through telephone, requesting response, or after a specified timeout has elapsed, security action (see Vaios, col. 8, lines 59-65).

Regarding claim 105, the combination shows the limitations of claim 92 as applied above, and further shows further comprising an external access control mechanism to said environment (see Vaios, col. 9, lines 61-64).

Regarding claim 109, the combination shows the limitations of claim 59 as applied above, and further shows where said environment is a home environment (see Vaios, col. 9, line 53).

Regarding claim 110, the combination shows the limitations of claim 59 as applied above, and further shows where said environment is a commercial environment (see Vaios, col. 9, line 52-53).

Regarding claim 112, the combination shows the limitations of claim 59 as applied above, and further shows wherein the at least one service includes a security monitoring service (see Vaios, col. 9, lines 49-64).

Regarding claim 113, the combination shows the limitations of claim 59 as applied above, and further shows wherein the at least one service includes a video surveillance service (see Vaios, col. 9, lines 49-64).

Regarding claim 114, the combination shows the limitations of claim 59 as applied above, and further shows wherein the at least one service includes an automation and control service (see Vaios, col. 9, lines 49-64).

Regarding claim 117, the combination shows the limitations of claim 59 as applied above, and further shows where the at least one service implements monitoring or control of a plurality of devices connected to at least one network interconnected with connection gateway (see Vaios, col. 9, lines 32-35).

Regarding claim 123, the combination shows the limitations of claim 59 as applied above, and further shows wherein the environment is a network separate from the extranet and the connection gateway serves as an entrance from the environment to the extranet (see Vaios, Fig. 1 and col. 4, lines 30-67)

Claims 60, 61, 63, 75, 85, and 86 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaios (US Patent No. 6,271,752) in view of Malkin (US Patent No. 6,061,650), and further in view of Barnier (US Patent No. 6,453,348) and Akatsu et al. (US Patent No. 6,496,862, hereinafter "Akatsu").

Regarding claim 60, the combination shows the limitations of claim 59 as applied above, but does not explicitly show wherein the connection gateway located in said environment is adapted to serve, in said communications session, a user interface for the control of the operation of the at least one service in accordance with operation instructions input via said Internet browser and the monitoring of the operation of the at least one service in said environment. Akatsu shows wherein the connection gateway located in said environment is adapted to serve, in said communications session, a user interface for the control of the operation of the at least



one service in accordance with operation instructions input via said Internet browser and the monitoring of the operation of the at least one service in said environment (see col. 19, lines 24-40). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaios with the teachings of Akatsu in order to reduce the burden on local computer 12.

Regarding claim 61, the combination shows the limitations of claim 60 as applied above, and further shows wherein said service includes monitoring and controlling is adapted to at least one of monitor and control, one or more devices interconnected with said connection gateway (see Akatsu, col. 19, lines 24-40 and Vaios, col. 8, lines 1-18).

Regarding claim 63, the combination shows the limitations of claim 61 as applied above, and further shows wherein at least one of said devices is a monitoring device located within said environment (see Vaios, col. 7, lines 39-61).

Regarding claim 75, the combination shows the limitations of claim 61 as applied above, and further shows wherein the connection gateway acts as a hub and Internet connection mechanism for said interconnected connected devices including information appliances (see Akatsu, col. 19, lines 24-40).

Regarding claim 85, the combination shows the limitations of claim 75 as applied above, and further shows wherein at least one of said devices comprises a digital security camera

embodying an image capture and compression method and an interconnection to said connection gateway (see Vaios, col. 9, lines 10-26).

Regarding claim 86, the combination shows the limitations of claim 85 as applied above, and further shows wherein said camera includes motion detection and image significance algorithms which run in said camera, and a filter so that only detected motion input is compressed and sent through said connection gateway to said extranet (see Vaios, col. 8, line 36 to col. 9, line 26).

Claims 69-71, 84, 107, 108, and 119 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaios (US Patent No. 6,271,752) in view of Malkin (US Patent No. 6,061,650), and further in view of Barnier (US Patent No. 6,453,348) and Tolopka et al. (US Patent No. 6,044,349, hereinafter "Tolopka").

Regarding claim 69, the combination shows the limitations of claim 59 as applied above, but does not explicitly show wherein said Internet browser runs on an Internet access device which includes a smartcard reader and associated user smartcard which provides authentication details and a URL corresponding to said environment. Tolopka shows a device which includes a smartcard reader and associated user smartcard which provides authentication details and a URL corresponding to an environment (see col. 2, lines 59-67 and col. 5, lines 1-13). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the

system of Vaios with the teachings of Tolopka in order to provide for additional security and convenience.

Regarding claim 70, the combination shows the limitations of claim 69 as applied above, and further shows wherein said smartcard also facilitates global access to the Internet for access of said extranet, and is adapted for additionally tracking connections for expenses (see Tolopka, col. 1, lines 43-46).

Regarding claim 71, the combination shows the limitations of claim 69 as applied above, and further shows wherein the Internet access device is a computer (see Vaios, col. 4, lines 5-14).

Regarding claim 84, the combination shows the limitations of claim 76 as applied above, but does not explicitly show wherein said control terminal is equipped with a smartcard reader for e-commerce transactions over said extranet. Tolopka shows wherein a terminal is equipped with a smartcard reader for e-commerce transactions over said extranet (see col. 1, lines 28-41. It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaios with the teachings of Tolopka in order to provide for additional security and convenience.

Regarding claim 107, the combination shows the limitations of claim 92 as applied above, but does not explicitly show further comprising a smartcard reader that is used for user authentication. Tolopka shows a smartcard reader that is used for user authentication (see col. 3,

lines 5-15). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaios with the teachings of Tolopka in order to provide for additional security and convenience.

Regarding claim 108, the combination shows the limitations of claim 107 as applied above, but does not explicitly show wherein a smartcard includes a biosensor attached to a substrate of the smartcard and interconnected with a circuit embedded in the smartcard to authenticate the user before the smartcard will operate. Tolopka shows wherein a smartcard includes a biosensor attached to a substrate of the smartcard and interconnected with a circuit embedded in the smartcard to authenticate the user before the smartcard will operate (see col. 3, lines 35-55). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaios with the teachings of Tolopka in order to provide for additional security and convenience.

Regarding claim 119, the combination shows the limitations of claim 59 as applied above, but does not explicitly show wherein the Internet browser runs on an Internet access device which includes a smartcard reader and associated user smartcard which provides authentication to access said predetermined address to create a connection to said environment. Tolopka shows an Internet access device which includes a smartcard reader and associated user smartcard which provides authentication to access said predetermined address to create a connection to said environment (see col. 2, lines 59-67 and col. 5, lines 1-13)+. It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the

system of Vaios with the teachings of Tolopka in order to provide for additional security and convenience.

Claim 72 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vaios (US Patent No. 6,271,752) in view of Malkin (US Patent No. 6,061,650), and further in view of Barnier (US Patent No. 6,453,348) and Woo et al. (US Patent No. 5,948,059, hereinafter "Woo").

Regarding claim 72, the combination shows the limitations of claim 59 as applied above, but does not explicitly show wherein the connection gateway detects a fax and stores the fax. Woo shows wherein a gateway detects a fax and stores the fax (see col. 4, lines 26-31). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaios with the teachings of Woo in order to provide for an additional means of data transmission.

Claim 73 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vaios (US Patent No. 6,271,752) in view of Malkin (US Patent No. 6,061,650), and further in view of Barnier (US Patent No. 6,453,348), Krehnke et al. (US Patent No. 6,014,746, hereinafter "Krehnke"), and Jones (US Patent No. 5,809,311).

Regarding claim 73, the combination shows the limitations of claim 59 as applied above, but does not explicitly show wherein the connection gateway is in a tamper proof enclosure, and operates without main power.

Krehnke shows a tamper proof enclosure (see col. 8, lines 26-40). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the

Jones shows a system which operates without main power (see col. 2, lines 23-35). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaios with the teachings of Jones in order to provide for continued operation in the event of a power failure.

Claim 74 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vaios (US Patent No. 6,271,752) in view of Malkin (US Patent No. 6,061,650), and further in view of Barnier (US Patent No. 6,453,348) and Krehnke (US Patent No. 6,014,746).

Regarding claim 74, the combination shows the limitations of claim 59 as applied above, but does not explicitly show wherein the connection gateway is tamper proof, and triggers an alarm and relays the alarm to the extranet in case of attempted tampering. Krehnke shows wherein a system is tamper proof, and triggers an alarm and relays the alarm to the extranet in case of attempted tampering (see col. 8, lines 26-40). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaios with the teachings of Krehnke in order to discourage interference from malicious individuals.

Claim 77 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vaios (US Patent No. 6,271,752) in view of Malkin (US Patent No. 6,061,650), and further in view of Barnier (US Patent No. 6,453,348) and Foster (US Patent No. 5,668,929).

Regarding claim 77, the combination shows the limitations of claim 76 as applied above, but does not explicitly show wherein the control terminal is equipped with biosensor, for access authentication of a local user in said environment to said connection gateway. Foster shows wherein a terminal is equipped with biosensor, for access authentication of a local user in said environment to said connection gateway (see col. 4, lines 56-63). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaios with the teachings of Foster in order to provide for additional security.

Claims 82 and 90 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaios (US Patent No. 6,271,752) in view of Malkin (US Patent No. 6,061,650), and further in view of Barnier (US Patent No. 6,453,348) and Nakamura et al. (US Patent No. 6,178,413, hereinafter "Nakamura").

Regarding claim 82, the combination shows the limitations of claim 76 as applied above, but does not explicitly show wherein the control terminal includes a personal computer (PC) equipped with a user premises network connection, wherein said PC runs a browser accessing a URL corresponding to said connection gateway. Nakamura shows wherein a terminal includes a personal computer (PC) equipped with a user premises network connection, wherein said PC runs a browser accessing a URL corresponding to a destination (col. 2, lines 1-19). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaios with the teachings of Nakamura in order comply with standard HTTP behavior.

Regarding claim 90, the combination shows the limitations of claim 89 as applied above, but does not explicitly show wherein said network address locators comprise Universal Resource Locators. Nakamura shows wherein said network address locators comprise Universal Resource Locators (col. 2, lines 1-19). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaios with the teachings of Nakamura in order to comply with standard HTTP behavior.

Claim 83 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vaios (US Patent No. 6,271,752) in view of Malkin (US Patent No. 6,061,650), and further in view of Barnier (US Patent No. 6,453,348) and Britt et al. (US Patent No. 5,940,074, hereinafter "Britt").

Regarding claim 83, the combination shows the limitations of claim 76 as applied above, but does not explicitly show wherein the control terminal is provided by a set top box connected to a television and running a web browser. Britt shows wherein a terminal is provided by a set top box connected to a television and running a web browser (see col. 4, lines 7-16). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaios with the teachings of Britt in order to provide access for users who own a television but not a computer.

Claim 87 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vaios (US Patent No. 6,271,752) in view of Malkin (US Patent No. 6,061,650), and further in view of Barnier (US Patent No. 6,453,348) and Lea et al. (US Patent No. 6,032,202, hereinafter "Lea").



Regarding claim 87, the combination shows the limitations of claim 59 as applied above, but does not explicitly show wherein said connection gateway provides support for at least one of the HomePnP, Bluetooth, HomeRF, Hiperlan and HAVi standard for network communication and appliance control. Lea shows wherein a gateway provides support for at least one of the HomePnP, Bluetooth, HomeRF, Hiperlan and HAVi standard for network communication and appliance control (see col. 6, lines 17-21). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaios with the teachings of Lea in order to support a wide variety of network protocols.

Claim 95 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vaios (US Patent No. 6,271,752) in view of Malkin (US Patent No. 6,061,650), and further in view of Barnier (US Patent No. 6,453,348) and Sadovnik et al. (US Patent No. 5,497,430, hereinafter "Sadovnik").

Regarding claim 95, the combination shows the limitations of claim 92 as applied above, but does not explicitly show wherein photos of authorized occupants of said environment are accessible from said extranet and are accessed upon said alarm event and cross referenced with said surveillance data to ascertain whether a true alarm condition has been raised. Sadovnik shows wherein photos of authorized occupants of an environment are accessible and are accessed upon said alarm event and cross referenced with said surveillance data to ascertain whether a true alarm condition has been raised (see col. 1, lines 19-40 and col. 5, lines 4-15). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaios with the teachings of Sadovnik in order to provide for additional security.

Claims 96-100 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaios (US Patent No. 6,271,752) in view of Malkin (US Patent No. 6,061,650), and further in view of Barnier (US Patent No. 6,453,348) and Swartz (US Patent No. 6,445,694).

Regarding claim 96, the combination shows the limitations of claim 92 as applied above, but does not explicitly show wherein the connection gateway incorporates a user programmed phone call answer strategy, including delayed answer, and upon answering said phone call, optionally detects a voice call, in which case it records a compressed version of the voice call for later retrieval by the user, thus operating in answering machine mode. Swartz shows wherein a system incorporates a user programmed phone call answer strategy, including delayed answer, and upon answering said phone call, optionally detects a voice call, in which case it records a compressed version of the voice call for later retrieval by the user, thus operating in answering machine mode (see col. 12, lines 36-59). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaios with the teachings of Swartz in order to provide for additional communications options.

Regarding claim 97, the combination shows the limitations of claim 96 as applied above, but does not explicitly show wherein upon answering an incoming call, the connection gateway raise a connection to a communications server, and sends an indication to the user of said security system of the receipt of a recorded message. Swartz shows wherein upon answering an incoming call, a system raises a connection to a communications server, and sends an indication to the user of said system of the receipt of a recorded message (see col. 12, lines 36-59). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify

the system of Vaios with the teachings of Swartz in order to provide for additional communications options.

Regarding claim 98, the combination shows the limitations of claim 92 as applied above, but does not explicitly show wherein said connection gateway sends a recorded compressed voice messages to a communications server for storage on said extranet for forwarding to a user of said environment. Swartz shows wherein a system sends a recorded compressed voice messages to a communications server for storage on said extranet for forwarding to a user of said environment (see col. 12, lines 36-59). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaios with the teachings of Swartz in order to provide for additional communications options.

Regarding claim 99, the combination shows the limitations of claim 92 as applied above, and further shows wherein said environment is a home environment (see Vaios, col. 9, line 53); but does not explicitly show wherein the connection gateway provides an indication of messages received on a HTML page accessible by a user of said home environment. Swartz shows wherein a system provides an indication of messages received on a HTML page accessible by a user of an environment (see col. 12, lines 36-59). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaios with the teachings of Swartz in order to provide for additional communications options.

Regarding claim 100, the combination shows the limitations of claim 92 as applied above, but does not explicitly show wherein said connection gateway is programmable to allow different response mechanisms to differing classes of alert event. Swartz shows wherein a system is programmable to allow different response mechanisms to differing classes of alert event (see col. 11, lines 1-20). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaios with the teachings of Swartz in order to provide for additional communications options.

Claim 101 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vaios (US Patent No. 6,271,752) in view of Malkin (US Patent No. 6,061,650), and further in view of Barnier (US Patent No. 6,453,348) and Coile et al. (US Patent No. 6,108,300, hereinafter "Coile").

Regarding claim 101, the combination shows the limitations of claim 92 as applied above, but does not explicitly show wherein said connection gateway contains connection details for preferred and secondary communications communication servers on said extranet, so that if a first communications communication server does not respond, other communications communication servers may be contacted until successful connection is achieved. Coile shows wherein a system contains connection details for preferred and secondary communications communication servers on said extranet, so that if a first communication server does not respond, other communication servers may be contacted until successful connection is achieved (see col. 3, line 66 to col. 4, line 22). It would have been obvious to one of ordinary skill in the art at the

time of the invention to further modify the system of Vaios with the teachings of Coile in order to provide for more reliability.

Claim 103 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vaios (US Patent No. 6,271,752) in view of Malkin (US Patent No. 6,061,650), and further in view of Barnier (US Patent No. 6,453,348) and Bruck et al. (US Patent No. 6,088,330, hereinafter "Bruck").

Regarding claim 103, the combination shows the limitations of claim 92 as applied above, but does not explicitly show wherein said user data storage on said extranet is allocated redundantly, ensuring integrity of stored surveillance data. Bruck shows wherein user data storage is allocated redundantly, ensuring integrity of stored surveillance data (see col. 2, lines 5-15). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaios with the teachings of Bruck in order to provide for more reliability.

Claim 106 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vaios (US Patent No. 6,271,752) in view of Malkin (US Patent No. 6,061,650), and further in view of Barnier (US Patent No. 6,453,348) and Koopman et al. (US Patent No. 5,649,014, hereinafter "Koopman").

Regarding claim 106, the combination shows the limitations of claim 92 as applied above, but does not explicitly show further comprising a reader for an RF tag embodied in keyfob or other device that is used for user authentication. Koopman shows a reader for an RF

tag embodied in keyfob or other device that is used for user authentication (see col. 1, lines 16-27). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaios with the teachings of Koopman in order to provide for additional security.

Claims 111, 115, and 116 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaios (US Patent No. 6,271,752) in view of Malkin (US Patent No. 6,061,650), and further in view of Barnier (US Patent No. 6,453,348) and Argyroudis (US Patent No. 5,892,758).

Regarding claim 111, the combination shows the limitations of claim 59 as applied above, but does not explicitly show where said environment is an industrial environment. Argyroudis shows an industrial environment (see col. 3, lines 7-20). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaios with the teachings of Argyroudis in order to provide for varied applications of the monitoring system.

Regarding claim 115, the combination shows the limitations of claim 59 as applied above, but does not explicitly show wherein the at least one service includes a utility metering service. Argyroudis shows wherein at least one service includes a utility metering service (see col. 3, lines 7-20). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaios with the teachings of Argyroudis in order to provide for varied applications of the monitoring system.

Regarding claim 116, the combination shows the limitations of claim 59 as applied above, but does not explicitly show wherein the at least one service includes an energy management service. Argyroudis shows wherein at least one service includes an energy management service (see col. 3, lines 7-20). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaios with the teachings of Argyroudis in order to provide for varied applications of the monitoring system.

Claim 118 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vaios (US Patent No. 6,271,752) in view of Malkin (US Patent No. 6,061,650), and further in view of Barnier (US Patent No. 6,453,348) and Kikinis (US Patent No. 6,243,596).

Regarding claim 118, the combination shows the limitations of claim 59 as applied above, but does not explicitly show where the Internet browser is on a mobile phone. Kikinis shows where an Internet browser is on a mobile phone (see col. 14, lines 64-65). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaios with the teachings of Kikinis in order to reduce the number of devices mobile users need to carry.

Claim 120 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vaios (US Patent No. 6,271,752) in view of Malkin (US Patent No. 6,061,650), and further in view of Barnier (US Patent No. 6,453,348) and Venkatraman et al. (US Patent No. 5,956,487, hereinafter "Venkatraman").

Regarding claim 120, the combination shows the limitations of claim 91 as applied above, but does not explicitly show wherein the connection gateway is embodied in a security camera. Venkatraman shows embodying network functionality in a security camera (see col. 2, lines 13-52). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaíos with the teachings of Venkatraman in order to reduce the number of devices necessary to implement the system.

Claim 124 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vaíos (US Patent No. 6,271,752) in view of Malkin et al. (US Patent No. 6,061,650, hereinafter “Malkin”).

Regarding claim 124, note that the preamble has been given patentable weight as it is relied upon by the body of the claim.

Vaíos shows a system for remote access of environments (surveillance areas 4: see col. 3, lines 24-27; col. 9, lines 32-35) comprising:

- an Internet browser (remote computer system 16: see col. 4, lines 5-7);
- a network located external to said environments environment and accessible via said Internet browser (communications network 6: see col. 4, lines 30-42);
- a plurality of connection gateways, each of said environments having located therein a different one or more of said connection gateways (network interfaces 14: see Fig. 1 and col. 3, lines 24-27).

Vaíos further shows controlling or monitoring operation of at least one service in said environment (see col. 7, lines 39-56, and col. 9, lines 49-61, with said connection gateway



providing access to information contained within the environment directly to said Internet browser (see col. 7, lines 39-56).

Vaios does not explicitly show:

- at least one communications server located in said network and adapted to interconnect on-demand with said connection gateways;
- wherein responsive to accessing a predetermined address by said Internet browser on said network, in which accessing said Internet browser provides authorization data, one of said at least one communications server subsequently:
  - determines which one of said environments said authorization data indicates authority to access; and
  - creates a new communications session between said communications server and one of said connection gateways, which is located in said environment, with said connection gateway subsequently providing access to information contained within the environment directly to said Internet browser.

Malkin shows:

- at least one communications server located in a network and adapted to interconnect on-demand with connection gateways (Remote Access Server 22: see col. 2, lines 13-17);
- wherein responsive to accessing a predetermined address by said Internet browser on said network (comprising the RAS's telephone number: see col. 3, lines 22-

25), in which accessing said Internet browser provides authorization data (see col. 3, lines 40-47), one of said at least one communications server subsequently:

- determines which one of said environments said authorization data indicates authority to access (comprising using the domain part of the login name to look up the address of a gateway interface and authentication server for a particular home network: see col. 3, line 48 to col. 4, line 14); and
- creates a new communications session between said communications server and one of said connection gateways (comprising a tunnel to a gateway: see col. 5, lines 35-46), which is located in said environment (see col. 5, line 65 to col. 6, line 3), with said connection gateway subsequently providing access to information contained within the environment directly to said Internet browser (see col. 6, lines 30-35).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Vaios with the communication server, authorization, and session establishment taught by Malkin in order to allow a user at a mobile remote node to seamlessly access his home environment (see Malkin, col. 1, lines 38-40).

#### **(10) Response to Argument**

The Examiner will address Appellant's arguments in the order they are presented in the Appeal Brief (hereinafter "the Brief").

A. Rejection of claims 59 to 61, 63 to 120, 123, and 124, under 35 USC § 112, ¶ 1

Beginning on page 7 of the Brief, Appellant argues in substance that the instant specification provides written description for the limitation "determines which one of said environments said authorization data indicates authority to access." The Examiner disagrees. Nowhere does the specification explicitly, implicitly, or inherently describe such a determination step.

First, the specification does not explicitly describe the claimed determination step. As explained in the Final Rejection, the most relevant part of the specification begins page 9, under the heading "Remote Operation." The user first authenticates to the provider network 17 by accessing a URL and providing a username and password associated with the URL (see p. 9, lines. 13-19). The provider network then retrieves "records associated with the user, detailing connection parameters for the user premises" (see p. 9, lines 22-24). However, provider network 17 retrieving records "detailing connection parameters" is not the same as the "at least one communication server...determin[ing] which one of said environments said authorization data indicates authority to access." Appellant points to several other portions of the specification, but neither these nor any other portions explicitly describe the claimed determination step. For example, lines 20-23 of p. 12 describe that "end point gateway 22 is programmed with the IP address specified in the connection profile." However, programming an end point gateway is not the same as a communications server determining which one of a set of environments authorization data indicates authority to access.

Second, the specification does not implicitly describe the claimed determination step. On the bottom of page 8 of the Brief, Appellant argues that, with respect to lines 20-23 of p. 12 of

the specification, “one of ordinary skill in the art would understand that the connection profile is not used to program the gateway with an IP address, but rather indicates with which IP address the gateway is programmed so that the communications server can establish the connection to the correct IP address of the relevant gateway.” In other words, Appellant appears to be arguing that the relevant gateway *already has been programmed* with the IP address specified in the “connection profile,” and the implication is that this IP address is then used to determine and contact the relevant gateway. The Examiner disagrees. The section of the specification that spans pp. 12-13 and is labeled “Case 1: Dynamic assignment is achieved by reconfiguration of end point router interface configuration tables service node 20” is clearly a list of *steps* described using the passive voice. This section describes an unspecified actor(s) that causes (1) a control channel *to be established*, (2) an end point gateway 22 *to be programmed* with the IP address, (3) a request for response *to be sent*, and so on. Thus, the IP address is not used (even impliedly) to *determine an environment*, as claimed, but rather to *program end point gateway 22*.

Third, the specification does not inherently describe the claimed determination step. In other words, the system described by the specification does not necessarily require that the determination is made based on “which one of said environments *said authorization data indicates authority to access*” (emphasis added). For example, the retrieved “records associated with the user, detailing connection parameters,” are not inherently used to determine an environment. Lines 5-8 of p. 10 describe that the gateway and a connection server “negotiate connection parameters”; the retrieved records may simply be used as a starting point for that negotiation, and not for a determination of an environment. This is consistent with lines 20-23 of p. 12, which describe that the end point gateway is “programmed...with the connection details

required to establish physical connection." Furthermore, as admitted by Appellant (see bottom of p. 8 of the Brief), particular URLs are provided which correspond to a user premises (i.e., "environments"). See also lines 7-34 on p. 9 of the specification. Indeed, far from requiring the authorization data to be used in the determination of the environment, the specification actually implies that this URL is used to determine the environment. Page 9 of the specification describes that "private Web pages are provided for each user (see line 9), and that a remote user can "view the private HTML pages that are dedicated to monitoring and control of the user premises by entering a URL associated with the HTML page they wish to access" (see lines 13-16). If the specification inherently required that the communication server "determines which one of said environments said authorization data indicates authority to access," the user would not need to enter a URL. Rather, the system would simply look up the appropriate URL using the username and password.

For the reasons given above, the Examiner maintains that the application as filed does not explicitly, implicitly, or inherently describe "at least one communications server" that "determines which one of said environments said authorization data indicates authority to access."

B. Rejection of claims 59, 64 to 68, 76, 78 to 81, 88, 89, 91 to 94, 102, 104, 105, 109, 110, 112 to 114, 117, and 123 under 35 U.S.C. § 103(a)

Beginning on p. 9 of the Brief, Appellant submits that Vaios, Malkin, and Barnier do not render obvious the claimed invention. The Examiner disagrees for the reasons presented below.

i. Claims 59, 64, 66 to 68, 76, 78 to 81, 88, 89, 91 to 94, 102, 104, 105, 109, 110, 112 to 114, 117, and 123

Beginning on p. 10 of the Brief, Appellant argues in substance that claim 59 and, by extension, its dependent claims rejected under the same grounds, are not obvious over the combination of Vaios, Malkin, and Barnier. The Examiner disagrees.

Applicant begins by arguing that the combination proffered by the Examiner would fail to function for technical reasons. Before addressing the particulars of Appellant's arguments, the Examiner wishes to provide some background as to how the references operate.

Like the instant invention, Vaios is directed to a system for remote surveillance of a plurality of environments, such as homes or businesses (see col. 3, lines 14-36 and col. 9, lines 32-35). Vaios provides an Internet browser to be used for surveillance (such as a web browser 138 running on remote computer system 16: see col. 4, lines 5-20 and col. 7, lines 39-56), and a network that is external to the environments and accessible via the Internet browser (communications network 6: see col. 4, lines 15-42). Connection to the environments is made by way of one of a plurality of connection gateways (including network interfaces 14), one of which is located in each of the environments (see col. 3, lines 24-27; col. 4, line 66 to col. 5, line 14; and col. 6, lines 54-67). The user accesses a predetermined address using the Internet browser (that is, accesses the remote site, which has a predetermined address, using the browser: see col. 4, lines 47-57 and col. 7, lines 39-56), provides authorization data (see col. 9, lines 60-64), and creates a new communications session (e.g., a surveillance session comprising a video feed, made over a telephone connection: see col. 4, lines 47-57 and col. 7, lines 39-56) with one of the gateways to control or monitor operation of at least one service in said environment (for

example, by providing the video feed and controls to manipulate the camera: see col. 7, lines 39-56 and col. 9, lines 49-61), with the gateway providing access to information contained within the environment directly to said Internet browser (e.g., providing the video feed to the browser: see col. 7, lines 39-56).

A difference between Vaios and the claimed invention is that Vaios does not use an intermediary “communications server” in the network to establish the connection, and does not use authorization data to determine which one of said environments said authorization data indicates authority to access. Malkin, by contrast, establishes connections by way of an intermediary communications server (the “Remote Access Server” or RAS: see col. 2, lines 13-30), and uses authorization data to determine which of a plurality of environments said authorization data indicates authority to access (that is, determines the address of a gateway for the user’s “home network”: see col. 2, lines 30-40). In Malkin, the user accesses a predetermined address on a network (the address of the RAS: see col. 3, lines 22-30), in which accessing the user provides authorization data (see col. 3, lines 40-47). The communications server uses the authorization data to look up an appropriate gateway (gateway 22: see col. 3, line 48 to col. 5, line 14), which corresponds to the user’s home network (home network 18: see col. 5, line 65 to col. 6, line 3), and establishes a session with that gateway (a tunnel: see col. 4, lines 58-65 and col. 5, lines 35-46).

A difference between Vaios, Malkin, and the claimed invention is that Vaios and Malkin do not provide for an extranet. Barnier, by contrast, provides for an extranet (see col. 2, lines 33-52). The extranet of Barnier is operable in an environment that makes use of telephone and/or Internet connections (see col. 4, lines 23-40 and col. 4, line 60 to col. 5, line 16).

Having established the Examiner's understanding of the cited references, the Examiner will now turn to the particulars of Appellant's arguments.

Appellant first argues, beginning at the bottom of p. 11, that "the SPN 14 of the Malkin reference cannot be modified to include an extranet and access thereto." The Examiner disagrees. Barnier explicitly describes that extranets can "couple a plurality of non-related organizations together with appropriate routing and traffic management capabilities" (see col. 1, lines 45-47), and further indicates that each subscriber to an extranet "may have its own intranet coupling various of its organizations, for example, in the form of a local area network" (see col. 4, lines 28-32). Given that Barnier contemplates extranets with such broad support for routing between nodes, Applicant has not provided a compelling reason for concluding that the system of Vaio in view of Malkin would cease to function when augmented with the security of an extranet.

Appellant next argues, beginning at the bottom of p. 11, that claim 59 "refers to where the communications server creates the communications session in response to accessing a predetermined address on the extranet by an Internet browser," so that a dial-in connection does not disclose this feature of claim 59" (emphasis in original). First, the Examiner submits that the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981).



In this case, Vaios provides for accessing a predetermined address by an Internet browser (that is, accesses the remote site, which has a predetermined address, using the browser: see col. 4, lines 47-57 and col. 7, lines 39-56) and creating a communications session to a particular environment (e.g., a surveillance session comprising a video feed, made over a telephone connection: see col. 4, lines 47-57 and col. 7, lines 39-56).

Malkin provides for accessing a predetermined address (the address of the RAS: see col. 3, lines 22-30), and a communications server responsively creating a communications session (a tunnel: see col. 4, lines 58-65 and col. 5, lines 35-46). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Vaios with the communication server, authorization, and session establishment taught by Malkin in order to allow a user at a mobile remote node to seamlessly and transparently access his home environment (see Malkin, col. 1, lines 38-40). Additionally, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Vaios with the communication server, authorization, and session establishment taught by Malkin in order to allow a user at a mobile remote node to access his home environment without the “tedious and burdensome task” of having to configure the remote node with the details of the connection (see Malkin, col. 3, lines 6-11).

Barnier provides for an extranet (see col. 2, lines 33-52). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaios with the extranet taught by Barnier in order to establish a highly secure environment in which to provide for monitoring (see Barnier, col. 4, lines 41-53).

Appellant next argues, on pp. 11-12 of the Brief, that Malkin “requires a dial-into the RAS 12 in order to distinguish, by the different open dial-in connections, between different remote nodes when decapsulating tunneled data.” Appellant goes on to argue, “the Malkin reference could not provide for the remote node to access another node on an extranet via an Internet browser using an extranet address...since the connection is not through dial-in, and the remote nodes have kept their local addresses.” Appellant still further argues that, in the combination, a “dial-in connection is required, contrary to claim 59.” First, the Examiner submits that both Vaios and Barnier provide for operation in systems that can make use of dial-in connections. See Vaios, col. 4, lines 47-57 and discussion of “dial-up access routers” in Barnier at col. 4, lines 35-40. Second, the Examiner notes that, in Malkin, multiple remote nodes are distinguished not by way of different dial-in connections, but by way of unique tunnel identifiers (see col. 5, lines 16-20). In other words, the tunneling taught by Malkin would continue to function even in the absence of a dial-in connection. Third, the Examiner submits that the claims do not exclude dial-in connections or accessing the address over a dial-in connection.

Appellant next argues, on p. 12 of the Brief, that Malkin does not provide for a communications server of one network to select a gateway of another network. The Examiner disagrees. First, claim 59 does not recite a network and another network, but “environments” and “an extranet located external to said environments.” The term “environment” is notably broader than the term “network,” and may be reasonably construed as encompassing the combination of home network 18 and gateway 22. Second, Malkin explicitly indicates that the gateway serves as the “home agent for the mobile node” and that the home agent is “a router *on a mobile node’s*

*home network*” (emphasis added; see col. 5, line 65 to col. 6, line 3). Third, the rejection is not based on Malkin alone, but on a combination including Vaios. Vaios clearly provides for a network external to environments (communications network 6, external to surveillance areas 4) and gateways located within the environments (network interfaces 14). See Fig. 1.

Appellant goes on to argue that “in figure 1, the Malkin reference clearly shows that gateway 22 belongs to the service provider network 14, and not the home network 18.” However, the circles drawn around the provider network and the home network in the figure are essentially logical distinctions between the networks. The mere fact that the circle labeled “service provider network 14” happens to include gateway 22 does not preclude gateway 22 from being part of the same “environment” as home network 18. Gateway 22 exists to forward data between the remote node and the elements on the home network, and thus may be reasonably included as part of the “environment” that also includes the home network.

Appellant next argues that “col. 5, ll. 6-11 of the Malkin reference clearly indicates that the gateway is a component external to the home network, that forwards data to the home network” (emphasis in original). Notably, however, the section cited by Appellant does not even mention the word “external.”

Appellant argues that “because the home agent is generally defined as a router which is on a home network, and the Malkin reference still describes the gateway as being separate from the home network, the Malkin reference teaches away from moving the gateway to the home network.” The Examiner disagrees. It is not clear how the section at issue (col. 5, line 65 to col. 6, line 3) discourages or otherwise discredits construing the home network and the home agent (gateway) as being part of the same environment.

Appellant next argues that the Examiner's position in the Advisory action is inconsistent with the claim, because "a node cannot be part of both the extranet and the environment, at least because by definition in the claim, a component of the extranet must be external to the environment." The Examiner disagrees. The claims require that the extranet, as a whole, be external to the environments, but do not preclude some node serving as a connection between the two.

Appellant next argues that the environment cannot be "arbitrarily drawn...to include the gateway 22, since gateway 22 is clearly also part of the SPN 14, which, according to claim 59, would have to be external to the environment if the SPN 14 is relied upon for disclosing the extranet." The Examiner disagrees. Again, the mere fact that the circle labeled "service provider network 14" happens to include gateway 22 does not preclude gateway 22 from being part of the same "environment" as home network 18. Gateway 22 exists to forward data between the remote node and the elements on the home network, and thus may be reasonably included as part of the "environment" that also includes the home network.

For the reasons given above and in the rejections, the Examiner maintains that the claimed invention is obvious over the combination of Vaios, Malkin, and Barnier.

ii. Claim 65

On page 14 of the Brief, Appellant submits that the combination of Vaios, Malkin, and Barnier does not teach or suggest that authentication to access said extranet is required only once per Internet browser session, as claimed in claim 65. The Examiner disagrees.

Appellant first argues that “the Malkin reference merely states that a tunnel lifetime is maintained for the duration of the remote connection, but does not address whether authentication is required.” The Examiner disagrees. Malkin clearly states that authentication is required before creating a tunnel (see col. 3, lines 32-47). Malkin then establishes the tunnel based on the authentication, and “Once the tunnel is established, the PPP authentication phase *is completed*” (emphasis added; see col. 5, lines 40-41). If authentication were required more than once per session, then the authentication phase would not be “completed” and the RAS would not “maintain the tunnel lifetime *for the duration of the remote connection*” (emphasis added; see col. 5, lines 47-50).

Appellant next argues that “the Malkin reference does not refer to an Internet browser session, but rather to a dial-in connection used for directing data to the remote node.” However, the rejection was not based on Malkin alone, but on Vaios, Malkin, and Barnier. Vaios, for example, teaches Internet browser sessions (e.g., a surveillance session comprising a video feed, made over a telephone connection: see col. 4, lines 47-57 and col. 7, lines 39-56) and that authentication may be required (see col. 9, lines 61-63). Furthermore, the Examiner notes that Barnier also teaches authentication in connection with an extranet (see col. 4, lines 40-58). It would have been obvious to one of ordinary skill in the art to apply the single authentication taught by Malkin to the Internet browser session taught by Vaios and the extranet taught by Barnier in order to avoid annoying users with excessive authentication prompts while still maintaining the security offered by an authentication system.

For the reasons given above and in the rejections, the Examiner maintains that the claimed invention is obvious over the combination of Vaios, Malkin, and Barnier.

C. Rejection of Claims 60, 61, 63, 75, 85, and 86 Under 35 U.S.C. § 103(a)

Appellant's arguments in connection with these claims rely upon the arguments already addressed above. The Examiner disagrees for the same reasons as given above.

D. Rejection of Claims 69 to 71, 84, 107, 108, and 119 Under 35 U.S.C. § 103(a)

Beginning on p. 15 of the Brief, Appellant submits that Vaios, Malkin, Barnier, and Tolopka do not render obvious the claimed invention. The Examiner disagrees for the reasons presented below.

i. Claims 69 to 71 and 119

On p. 15, Appellant begins by reiterating the arguments made in connection with claim 59. The Examiner again disagrees.

Vaios provides for accessing a predetermined address by an Internet browser (that is, accesses the remote site, which has a predetermined address, using the browser: see col. 4, lines 47-57 and col. 7, lines 39-56) and creating a communications session to a particular environment (e.g., a surveillance session comprising a video feed, made over a telephone connection: see col. 4, lines 47-57 and col. 7, lines 39-56).

Malkin provides for accessing a predetermined address (the address of the RAS: see col. 3, lines 22-30), and a communications server responsively creating a communications session (a

tunnel: see col. 4, lines 58-65 and col. 5, lines 35-46). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Vaios with the communication server, authorization, and session establishment taught by Malkin in order to allow a user at a mobile remote node to seamlessly and transparently access his home environment (see Malkin, col. 1, lines 38-40). Additionally, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Vaios with the communication server, authorization, and session establishment taught by Malkin in order to allow a user at a mobile remote node to access his home environment without the “tedious and burdensome task” of having to configure the remote node with the details of the connection (see Malkin, col. 3, lines 6-11).

Barnier provides for an extranet (see col. 2, lines 33-52). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Vaios with the extranet taught by Barnier in order to establish a highly secure environment in which to provide for monitoring (see Barnier, col. 4, lines 41-53).

Turning now to the Tolopka reference, and its applicability to claim 69, Appellant argues that “because a dial-in connection would be required by the system provided by the combination of the Vaios, Malkin, and Barnier references, one of ordinary skill in the art would not have modified the system of the combination of the Vaios, Malkin, and Barnier references to include a smartcard with a URL corresponding to the environment as provided for in claim 69.” The Examiner disagrees. Even assuming, *arguendo*, that the combination requires a dial-in connection, it is not clear why such a connection prevents the inclusion of a smartcard with a URL corresponding to the environment. Tolopka provides generally for a system that is used to

disseminate information. A smartcard contains an address (such as a URL or telephone number) as well as the credentials necessary to access that address. See col. 2, lines 59-67 and col. 5, lines 1-26. The information located at the address can be “virtually any information” (see col. 8, lines 15-41). Thus, including the smartcard system of Tolopka in the combination of Vaios, Malkin, and Barnier would provide for secure, convenient access to information useful to the user in connection with the environment (see Tolopka, col. 1, line 61 to col. 2, line 2).

Appellant next argues, with respect to claim 119, that the allegedly required “dial-in” connection prevents the combination with Tolopka’s smart card reader. However, even assuming, *arguendo*, that the combination requires such a connection, the Examiner notes that Tolopka provides for an address comprising a telephone number, and the credentials required to access that number (see col. 5, lines 1-26).

For the reasons given above and in the rejections, the Examiner maintains that the claimed invention is obvious over the combination of Vaios, Malkin, Barnier, and Tolopka.

E. Rejection of Claim 72 Under 35 U.S.C. § 103(a)

Appellant’s arguments in connection with this claim rely upon the arguments already addressed above. The Examiner disagrees for the same reasons as given above.

F. Rejection of Claim 73 Under 35 U.S.C. § 103(a)

Appellant’s arguments in connection with this claim rely upon the arguments already addressed above. The Examiner disagrees for the same reasons as given above.



G. Rejection of Claim 74 Under 35 U.S.C. § 103(a)

Appellant's arguments in connection with this claim rely upon the arguments already addressed above. The Examiner disagrees for the same reasons as given above.

H. Rejection of Claim 77 Under 35 U.S.C. § 103(a)

Appellant's arguments in connection with this claim rely upon the arguments already addressed above. The Examiner disagrees for the same reasons as given above.

I. Rejection of Claims 82 and 90 Under 35 U.S.C. § 103(a)

Appellant's arguments in connection with these claims rely upon the arguments already addressed above. The Examiner disagrees for the same reasons as given above.

J. Rejection of Claim 83 Under 35 U.S.C. § 103(a)

Appellant's arguments in connection with this claim rely upon the arguments already addressed above. The Examiner disagrees for the same reasons as given above.

K. Rejection of Claim 87 Under 35 U.S.C. § 103(a)

Appellant's arguments in connection with this claim rely upon the arguments already addressed above. The Examiner disagrees for the same reasons as given above.

L. Rejection of Claim 95 Under 35 U.S.C. § 103(a)

Appellant's arguments in connection with this claim rely upon the arguments already addressed above. The Examiner disagrees for the same reasons as given above.

M. Rejection of Claims 96 to 100 Under 35 U.S.C. § 103(a)

Appellant's arguments in connection with these claims rely upon the arguments already addressed above. The Examiner disagrees for the same reasons as given above.

N. Rejection of Claim 101 Under 35 U.S.C. § 103(a)

Appellant's arguments in connection with this claim rely upon the arguments already addressed above. The Examiner disagrees for the same reasons as given above.

O. Rejection of Claim 103 Under 35 U.S.C. § 103(a)

Appellant's arguments in connection with this claim rely upon the arguments already addressed above. The Examiner disagrees for the same reasons as given above.

P. Rejection of Claim 106 Under 35 U.S.C. § 103(a)

Appellant's arguments in connection with this claim rely upon the arguments already addressed above. The Examiner disagrees for the same reasons as given above.

Q. Rejection of Claims 111, 115, and 116 Under 35 U.S.C. § 103(a)

Appellant's arguments in connection with these claims rely upon the arguments already addressed above. The Examiner disagrees for the same reasons as given above.

R. Rejection of Claim 118 Under 35 U.S.C. § 103(a)

Appellant's arguments in connection with this claim rely upon the arguments already addressed above. The Examiner disagrees for the same reasons as given above.

S. Rejection of Claim 120 Under 35 U.S.C. § 103(a)

Appellant's arguments in connection with this claim rely upon the arguments already addressed above. The Examiner disagrees for the same reasons as given above.

T. Rejection of Claim 124 Under 35 U.S.C. § 103(a)

Beginning on p. 22 of the Brief, Appellant argues that Vaio and Malkin do not render obvious the claimed invention. The Examiner disagrees. First, the Examiner notes that claim 124 is similar to claim 59, but uses the broader term "network" instead of the term "extranet." Thus, the Examiner submits that the arguments made above in connection with claim 59 apply with equal force to claim 124.

Appellant again begins by arguing that the combination requires a dial-in connection, because "the data is provided to the correct remote node using the open dial-in connection as a 'care-of' address" and "the dial-in connection is necessary for proper routing of the data to the correct remote node." Appellant goes on to argue that "Otherwise, if the remote node's address would be used instead, there can be collision between different data intended for different remote nodes." Appellant's argument is unclear. Specifically, it is not clear exactly what in the combination would result in collisions. It is true that an embodiment of Malkin makes use of

dial-in connections, but these connections are not used to distinguish between remote nodes. Rather, multiple remote nodes are distinguished by way of unique tunnel identifiers (see col. 5, lines 16-20). In other words, even assuming, *arguendo*, the tunneling taught by Malkin would function even without a dial-in connection. In fact, Malkin provides for the tunneling functionality where “link-layer connectivity to a point of attachment is available” (see col. 5, lines 58-63). As is understood in the art, such connectivity need not be over a dial-in connection.

Appellant next argues that a dial-in connection is “contrary to claim 124.” First, it is not clear why a dial-in connection is “contrary to claim 124.” Nothing in the claim excludes accessing the address over a dial-in connection. The claim requires accessing a predetermined address by an Internet browser on a network. Vaios provides for an Internet browser on a network accessing a predetermined address (in other words, the user accesses the remote site, which has a predetermined address, using the browser: see col. 4, lines 47-57 and col. 7, lines 39-56). As explained in Vaios, this connection can occur over a dial-in connection or any other network connection (see col. 4, lines 30-65).

Appellant still further argues that “the cited references provide no suggestion whatsoever to apply the set-up of the Malkin reference also to a case where a remote node uses a different address than its local network address of its home network.” It is not clear why the address of the remote node in the combination must be different from its local address. Malkin provides that a system allowing the node to retain its address is actually beneficial to the user, in that it relieves the user from the “tedious and burdensome task” of configuring the remote node (see col. 3, lines 6-11). Notably, Vaios indicates that “the browser and application software of the remote computer system may be *configured* to communicate with the local computer system” (see col. 2,

lines 41-45). Thus, implementing the automatic configuration of Malkin into the system of Vaios would make this configuration easier.

Finally, Appellant argues that the combination of references does not teach or suggest “these features of a gateway located in an environment external to which the network is located.” The Examiner disagrees. First, the term “environment” is extremely broad, and may be reasonably construed as encompassing the combination of home network 18 and gateway 22 of Malkin. Second, Malkin explicitly indicates that the gateway serves as the “home agent for the mobile node” and that the home agent is “a router *on a mobile node’s home network*” (emphasis added; see col. 5, line 65 to col. 6, line 3). Third, the rejection is not based on Malkin alone, but on a combination including Vaios. Vaios clearly provides for a network external to environments (communications network 6, external to surveillance areas 4) and gateways located within the environments (network interfaces 14). See Fig. 1.

For the reasons given above and in the rejections, the Examiner maintains that the claimed invention is obvious over the combination of Vaios and Malkin.

#### **(11) Related Proceeding(s) Appendix**

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner’s answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,  
  
/Christopher Biagini/  
  
Examiner, Art Unit 2442

Conferees:  
  
/Philip C Lee/  
  
Acting SPE of Art Unit 2442

/Jeffrey Pwu/  
  
Supervisory Patent Examiner, Art Unit 2446